UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,687	12/22/2000	Xun Wilson Huang	21816-04953	4655

7590 05/04/2005

JEFFREY BRILL
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
ZHEN, LI B	

ART UNIT	PAPER NUMBER
2194	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,687	HUANG ET AL.	
	Examiner	Art Unit	
	Li B. Zhen	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/04, 12/04, 2/05*. 4/05
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 58 are pending in the current application.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 8, 2005 has been entered.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1 – 20 are rejected under 35 U.S.C. 101 because they are directed to non-statutory subject matter.

5. Claims 1 – 20 are directed to method steps which can be practiced mentally in conjunction with pen and paper, therefore they are directed to non-statutory subject matter. Specifically, as claimed, it is uncertain what performs each of the claimed method steps. Moreover, each of the claimed steps, inter alia, designating, intercepting, granting, allowing, withdrawing, assigning, storing, identifying, terminating, loading, saving, and replacing, can be practiced mentally in conjunctions with pen and paper.

The claimed steps do not define a machine or computer implemented process [see MPEP 2106]. Therefore, the claimed invention is directed to non-statutory subject matter. (The examiner suggests applicant to change "method" to "computer implemented method" in the preamble to overcome the outstanding 35 U.S.C. 101 rejection).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1, 3 - 8, 13 - 16, 18, 21, 23 - 28, 33 - 36, 38, 41, 43 - 48, 53 - 56 and 58 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,961,582 to Gaines in view of U.S. Patent No. 6,449,652 to Blumenau et al. [hereinafter referred to as Blumenau].**

8. As to claim 1, Gaines teaches the invention substantially as claimed including a method for virtualizing user privileges [virtual permission; col. 6, lines 37 – 47] in a computer operating system [col. 13, lines 48 – 62] including multiple virtual processes [col. 6, lines 56 – 67], the method comprising:

designating a virtual user [user 201; col. 10, lines 16 – 28], the virtual user being associated with a virtual process [user 201 directs the remote computer 202 to send a

set of program code 207 for a virtual application 143; col. 10, lines 46 – 52 and col. 11, lines 42 – 57], wherein the virtual process is a plurality of actual processes [virtual process model 152 includes a set of actual processes 124; col. 6, lines 56 - 67];

intercepting a system call for which actual user privileges are required [The process control filter 151 scrutinizes a request for service to determine if the virtual application 143 requesting service has virtual permissions 147 to access to affect the virtual process 153 it seeks to access; col. 7, lines 1 – 15]; and

in response to the intercepted system call being made by a virtual user and pertaining to the virtual process of the virtual user [Each copy of the virtual operating system 141 has a unique identifier 209 that may be used to determine whether the program code 207 (and virtual application 143) has virtual permissions 147 to be executed; col. 11, lines 17 – 25]:

allowing execution of the system call [After determining that access should be allowed, the process control filter 151 translates the request for service into one or more direct calls on the application interface 111, requesting a like service from the operating system 103; col. 7, lines 1 - 15].

9. Although Gaines teaches virtual permissions [col. 6, lines 37 – 47], Gaines does not specify the permission as super-user permissions.

However, Blumenau teaches virtualizing super-user permissions [enable an application program to access a raw device, even though the application program does not have system administrator privileges; col. 7, lines 10 – 33] for access to virtual resources [file system 36 interprets each logical volume presented to it by the storage

system 3 as a single logical device, also referred to as a raw storage device; col. 8, line 56 – col. 9, line 12], intercepting a system call for which actual super-user privileges are required [a facility is implemented that intercepts all requests for access to a raw storage device; col. 11, lines 19 – 39], granting actual super-user privileges [security driver 42 modifies the "open file" request to indicate that the maker of the request is a user having system administrator privileges; col. 10, lines 13 – 29 and col. 11, lines 20 – 39], and allowing execution of the system call [col. 13, lines 31 – 60].

10. It would have been obvious to a person of ordinary skill in the art at the time of the invention to apply the teaching of virtualizing super-user permissions as taught by Blumenau to the invention of Gaines because this enables application programs to access raw devices without requiring that the applications be given system administrator privileges such that the privileges granted to any particular application program can be controlled and an application program can be restricted in the raw devices for which access is granted, as well as for the types of operations (e.g., read or write) that it can perform to particular raw devices [col. 7, lines 45 - 55 of Blumenau].

11. As to claim 3, Gaines as modified teaches assigning a virtual super-user identifier to the virtual super-user [col. 11, lines 18 – 23 of Gaines].

12. As to claim 4, Gaines as modified teaches the virtual super-user identifier comprises a super-user identifier and an indication of the virtual process [col. 12, lines 5 – 25 of Blumenau].

13. As to claim 5, Gaines as modified teaches assigning a user identifier to the virtual super-user and storing the user identifier and an indication of the virtual process of the virtual super-user in a virtual super-user list [col. 13, line 58 – col. 14, line 16 of Blumenau].

14. As to claim 6, Gaines as modified teaches assigning a super-user identifier to the virtual super-user [col. 11, lines 41 – 52 of Blumenau].

15. As to claim 7, Gaines as modified teaches the intercepted system call comprises a system call for accessing a file [col. 4, lines 23 – 39 of Gaines].

16. As to claim 8, Gaines as modified teaches the intercepted system call pertains to the virtual process of the virtual super-user when the file to be accessed is associated with the virtual process [col. 5, line 65 – col. 6, line 8 of Gaines].

17. As to claim 13, Gaines as modified teaches the system call is made by the virtual super-user when a user making the call has a virtual super-user identifier [col. 11, lines 41 – 52 of Blumenau].

18. As to claim 14, Gaines as modified teaches the system call is made by the virtual super-user when a user making the call has a user identifier in a virtual super-user list [col. 13, line 58 – col. 14, line 16 of Blumenau].

19. As to claims 15, Gaines as modified teaches responsive to the intercepted system call not being made by the virtual super-user, disallowing execution of the system call [col. 7, lines 1 – 13 of Gaines].

20. As to claim 16, Gaines as modified teaches responsive to the intercepted system call being made by the virtual super-user and not pertaining to the virtual process of the virtual super-user, disallowing execution of the system call [col. 7, lines 1 – 13 and col. 7, line 62 – col. 8, line 3 of Gaines].

21. As to claim 18, Gaines as modified teaches allowing comprises: executing the system call [col. 7, lines 1 – 15 of Gaines].

22. As to claims 21, 23 – 28, 33 – 36 and 38, these are product claims that correspond to method claims 1, 3 – 8, 13 – 16 and 18; note the rejections to claims 1, 3 – 8, 13 – 16 and 18 above, which also meet these product claims.

23. As to claims 41, 43 – 48, 53 – 56 and 58, these are system claims that correspond to method claims 1, 3 – 8, 13 – 16 and 18; note the rejections to claims 1, 3 – 8, 13 – 16 and 18 above, which also meet these systems claims.

24. **Claims 2, 22 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaines in view of Blumenau further in view of U.S. Patent NO. 6,578,055 to Hutchison [cited in previous office action].**

25. As to claims 2, 22 and 42, Gaines as modified teaches super-user privileges are granted on a per command basis [col. 5, lines 40 – 52 of Blumenau] but do not specifically teach withdrawing the actual super-user privileges from the virtual super-user after execution of the system call.

However, Hutchison teaches virtualizing super-user privileges in a computer operating system [a user level field of a data structure associated with the communication may be set to specify a root user level, such as 0; col. 3, lines 5 – 11], intercepting a system call for which actual super-user privileges are required [accesses to a file system are intercepted (block 200), Fig. 5; col. 8, lines 25 – 45], granting actual super-user privileges to the virtual super-user [the user level identified in the data structure accompanying the access is modified to the privileged user level, such as by setting the user level field to 0 (block 206), Fig. 5; col. 8, lines 43 – 54], allowing execution of the system call [access with the modified data structure is then forwarded to the file system (block 208), Fig. 5; col. 8, lines 43 – 54], and withdrawing the actual super-user privileges from the virtual super-user after execution of the system call [when the file mirroring operation completes (block 104) the privileged user level may be released (block 106); col. 8, lines 23 – 45].

26. It would have been obvious to a person of ordinarily skilled in the art at the time of the invention to apply the teaching of withdrawing the actual super-user privileges from the virtual super-user after execution of the system call as taught by Hutchison to the invention of Gaines as modified because this provides privileged user level only

when needed and reduces the risk of having a process at the root user level [col. 8, lines 23 – 31 of Hutchison].

27. **Claims 9 – 12, 17, 19, 20, 29 – 32, 37, 39, 40, 49 – 52 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaines in view of Blumenau further in view of U.S. Patent NO. 6,658,571 to O'Brien [cited in previous office action].**

28. As to claim 9, Gaines as modified does not teach terminating a process.

However, O'Brien teaches a system call wrapper intercepting system calls from applications [mechanism for dynamically wrapping standard, commercially available software application; col. 2, lines 10 – 39], invoking one or more security modules to process the system call [col. 2, lines 28 – 36], and a system call to terminate a process [close module 411 releases all the kernel buffers that were acquired and unregisters security module 105; col. 6, lines 17 – 36].

29. It would have been obvious to a person of ordinarily skilled in the art at the time of the invention to apply the teaching of a system call to terminate a process as taught by O'Brien to the invention of Gaines as modified because this allows a process and its resources to be released when the process is no longer needed [release all the kernel buffers; col. 6, lines 30 – 32 of O'Brien].

30. As to claim 10, Gaines as modified teaches the intercepted system call pertains to the virtual process of the virtual super-user when the process to be terminated is

associated with the virtual process [a security module 105 unregisters itself via the API, security master 103 removes it from list 207; col. 5, lines 1 – 27 of O'Brien].

31. As to claim 11, Gaines as modified teaches identifying each process associated with the virtual process [close module 411 releases all the kernel buffers that were acquired and unregisters security module 105; col. 6, lines 17 – 36 of O'Brien], and terminating each identified process [a security module 105 unregisters itself via the API, security master 103 removes it from list 207; col. 5, lines 1 – 27 of O'Brien].

32. As to claim 12, Gaines as modified teaches a data structure stores associations between processes and virtual processes, and identifying each process by its association with the virtual process in the data structure [file system 36 stores access privileges information for each of the logical volumes; col. 9, lines 1 – 12 of Blumenau].

33. As to claim 17, Gaines as modified teaches responsive to the intercepted system call comprising a system call for inserting a module [malicious software] into an operating system kernel, disallowing execution of the system call [each security module 105 "wraps" one or more applications 107 in the sense that applications 107 cannot access computing resources 106 for which they are unauthorized in the event that an application 107 executes malicious software; col. 3, lines 39 – 56 of O'Brien].

34. As to claim 19, Gaines as modified teaches loading a system call wrapper [Security modules 105 are kernel-loadable modules that make and enforce application-

specific or resource-specific policy decisions for applications 107; col. 3, lines 38 – 56 of O'Brien], saving a pointer to the system call [each entry includes the following fields: a pointer to the original system call handler within the operating system; col. 5, lines 27 – 46 of O'Brien] and replacing the pointer to the system call with a pointer to the system call wrapper, such that the system call wrapper is executed when the system call is invoked [for each system call being wrapped, security master 103 redirects each pointer from the standard handler within the operating system to a corresponding system call wrapper within security master 103; col. 5, lines 27 – 46 of O'Brien].

35. As to claim 20, Gaines as modified teaches the pointer to the first system call comprises a system call vector [Conventional operating systems include a system call table (ST) that contains pointers to handlers for the various system calls; col. 5, lines 28 – 46 of O'Brien].

36. As to claims 29 – 32, 37, 39 and 40, they are rejected for the same reasons as claims 9 – 12, 17, 19 and 20 above.

37. As to claims 49 – 52 and 57, they are rejected for the same reasons as claims 9 – 12, and 17 above.

Conclusion

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (571) 272-3768. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Li B. Zhen
Examiner
Art Unit 2194

lbz

SUE LAO
PRIMARY EXAMINER